

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-253241

(43)Date of publication of application : 14.09.2000

(51)Int.Cl.

H04N	1/40
G03G	21/04
G06F	3/12
G06F	12/00
G06F	13/00

(21)Application number : 11-049997

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 26.02.1999

(72)Inventor : KOJIMA AKIO
KUWABARA YASUHIRO
WATANABE TATSUMI

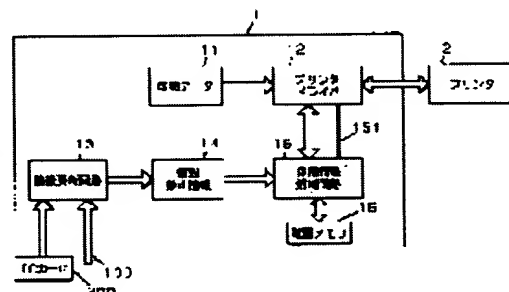
(54) DATA MONITORING METHOD AND DEVICE THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To previously and speedily prevent the illegal copy of electronic data whose copy is inhibited by stopping or preventing a copy operation when a development image is considered to be copy inhibition information.

SOLUTION: A printing information analysis circuit 15 always monitors printing data 11 transferred to a printer 2, previously forms character string information, picture pattern information and code information, which are filled by page description language as objective data and password information buried by electronic watermark technology into a final development image in a recognition memory 16 and collates it with information from copy inhibition information 14 so as to analyze it. When printing information is decided to be previously registered in copy inhibition information 14, a stop instruction 151 for stopping the transfer of printing data is outputted to a printer driver 12. The content of copy inhibition information 14 can always correspond to a content whose printing is to be inhibited and it can be updated.

Speedy correspondence to a security management level and security information, which are changed every day, can be executed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-253241

(P2000-253241A)

(43)公開日 平成12年9月14日(2000.9.14)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 N 1/40		H 0 4 N 1/40	Z 2 H 0 3 4
G 0 3 G 21/04		G 0 6 F 3/12	C 5 B 0 2 1
G 0 6 F 3/12		12/00	5 2 0 E 5 B 0 8 2
12/00	5 2 0	13/00	3 5 4 Z 5 B 0 8 9
13/00	3 5 4	G 0 3 G 21/00	5 5 2 5 C 0 7 7
審査請求 未請求 請求項の数20 O L (全 14 頁)			

(21)出願番号 特願平11-49997

(22)出願日 平成11年2月26日(1999.2.26)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 小嶋 章夫

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 ▲くわ▼原 康浩

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74)代理人 100097445

弁理士 岩橋 文雄 (外2名)

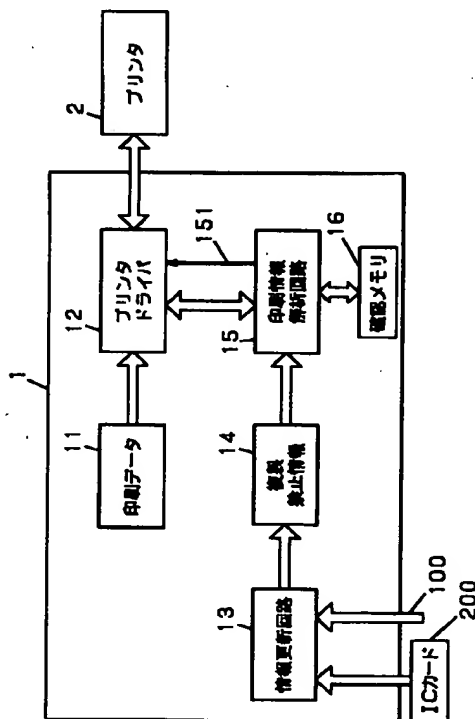
最終頁に続く

(54)【発明の名称】 データ監視方法、およびデータ監視装置

(57)【要約】

【課題】 迅速に、不正な複製を未然に防ぐことができるデータ監視方法。

【解決手段】 パーソナルコンピュータ1からプリンタ2にプリンタドライバ12を経由して印刷データ11を転送する際、印刷情報解析回路15が印刷データ11をモニターし、確認メモリ16で展開像を確認しながら、複製禁止情報14からの情報と照合および解析を行なう。もし、この印刷データ11の展開像が予め複製禁止情報14に登録されているものと判定した場合は、プリンタドライバ12に指示してプリンタ2への印刷データの転送を停止させる。これによって、不正な複製データをプリンタ2に出力する前に防止する。



【特許請求の範囲】

【請求項 1】 像形成可能な対象データと、複製が禁止されているデータ情報よりなる複製禁止情報と、前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、前記対象データの複製を生成する複製手段とを具備し、前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないことを特徴とするデータ監視方法。

【請求項 2】 前記データ監視方法は、更に、複製が禁止されているデータの複製禁止情報を更新する更新手段を具備し、複製禁止情報の変更ができることを特徴とする請求項 1 記載のデータ監視方法。

【請求項 3】 前記データ監視方法は、更に、変更権限の管理情報をもつ更新情報を取得する取得手段を備し、更新情報の内容に応じて、複製禁止情報の変更ができることを特徴とする請求項 2 記載のデータ監視方法。

【請求項 4】 前記更新情報は、記憶メディアによって提供されることを特徴とする請求項 3 記載のデータ監視方法。

【請求項 5】 前記更新情報は、認証確認ができる情報提供媒体によって提供されることを特徴とする請求項 3 記載のデータ監視方法。

【請求項 6】 前記更新情報は、ネットワークによって提供されることを特徴とする請求項 5 記載のデータ監視方法。

【請求項 7】 前記データ監視方法は、更に、他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、更新情報の履歴を保存する履歴保存手段と、を有し、他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更新することを特徴とする請求項 2 記載のデータ監視方法。

【請求項 8】 前記データ監視方法は、更に、前記データ監視手段の機能を停止させる解除手段を具備し、認証確認後に複製を停止させる機能を解除できることを特徴とする請求項 1 記載のデータ監視方法。

【請求項 9】 像画像を入力する入力手段と、前記像画像を監視するデータ監視手段と、他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段と、を具備し、前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させる又は行わないことを特徴とするデータ監視方法。

【請求項 10】 前記データ監視方法は、ネットワーク上の所定の装置に蓄積された複製禁止情報を問い合わせ

せ、取得することを特徴とする請求項 7 記載のデータ監視方法。

【請求項 11】 像形成可能な対象データと、複製が禁止されているデータ情報よりなる複製禁止情報と、前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、前記対象データの複製を生成する複製手段と、前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないように制御する制御手段と、を具備することを特徴とするデータ監視装置。

【請求項 12】 前記データ監視装置は、更に、複製が禁止されているデータの複製禁止情報を更新する更新手段を具備し、複製禁止情報の変更ができることを特徴とする請求項 11 記載のデータ監視装置。

【請求項 13】 前記データ監視装置は、更に、変更権限の管理情報をもつ更新情報を取得する取得手段を備し、更新情報の内容に応じて、複製禁止情報の変更を行うことを特徴とする請求項 12 記載のデータ監視装置。

【請求項 14】 前記更新情報は、記憶メディアによって提供されることを特徴とする請求項 13 記載のデータ監視装置。

【請求項 15】 前記更新情報は、認証確認ができる情報提供媒体によって提供されることを特徴とする請求項 13 記載のデータ監視装置。

【請求項 16】 前記更新情報は、ネットワークによって提供されることを特徴とする請求項 15 記載のデータ監視装置。

【請求項 17】 前記データ監視装置は、更に、他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、更新情報の履歴を保存する履歴保存手段と、を有し、他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更新することを特徴とする請求項 12 記載のデータ監視装置。

【請求項 18】 前記データ監視装置は、更に、前記データ監視手段の機能を停止させる解除手段を具備し、認証確認後に複製を停止させる機能を解除できることを特徴とする請求項 11 記載のデータ監視装置。

【請求項 19】 像画像を入力する入力手段と、前記像画像を監視するデータ監視手段と、他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段と、を具備し、前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させる又は行わないことを特徴とするデータ監視装置。

【請求項 20】 前記データ監視装置は、ネットワーク

上の所定の装置に蓄積された複製禁止情報を問い合わせ、取得することを特徴とする請求項 17 記載のデータ監視装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機密文書、機密データ、著作権物など複製が禁止された機密データ、文書、動画像、印刷物、紙幣や有価証券または各種金券等に対し、不正な複製を防止するデータ監視方法、及びその装置に関するものである。

【0002】

【従来の技術】近年、ネットワーク化、デジタル化の進展によって、個々の機器がネットワークに接続されて、電子データを手軽に取得、印刷できるようになってきた。一方、DTPでは作成原稿データに忠実な画像形成を目的として技術開発が進められた結果、高精細な複製物が得られるようになってきた。これによって、電子データを取得し、高精細な印刷が簡単にできる環境が整いつつある。

【0003】一方で機密管理された文書に対しては複製されると機密漏洩等問題になる。また、オリジナル原稿と区別がつかない複製物が簡単に得られると、著作権物の不正使用、さらには、紙幣や有価証券など偽造に悪用される恐れがあり、被害が大きい。

【0004】従来より、カラー複写機には紙幣等に対し偽造防止機能が搭載されていた。図 13 は従来のカラー複写機のブロック図である。図 13 において、スキャナ 110 から読み込まれた画像信号は、特定画像判定回路 120 によって複写が禁止されている紙幣や証券類の画像信号かどうかを画像特徴より判別し、縮小画像、鏡像反転などの変換処理を行ってから画像を再生したりする複写防止機能を起動することにより、複写物が容易に偽造物とわかる処理をしてプリンタ 130 に出力し、偽造を防止していた（例えば、特開平 1-316783 の画像処理装置）。

【0005】

【発明が解決しようとする課題】近年の傾向として紙による原稿だけでなく、電子化された文書の普及も目まじしい。パーソナルコンピュータによって、ネットワーク上から簡単に機密電子文書、著作権物データを入手し、高速プリンタで大量に不正印刷できるという課題がある。

【0006】ところで、上記先行技術は、スキャナから読み取られた原稿の画像を判別するものであるので、スキャナから読み取られない電子データに係る上記課題には対処できない。

【0007】本発明は、上記課題を解決するもので、複製が禁止された電子データの不正な複製を未然に、かつ迅速に防止するデータ監視法を提供することを目的とする。

【0008】

【課題を解決するための手段】上記課題を解決するために、本発明における第 1 のデータ監視方法は、像形成可能な対象データと、複製が禁止されているデータ情報よりなる複製禁止情報と、前記複製禁止情報に基づいて前記対象データから生成される展開像を監視するデータ監視手段と、前記対象データの複製を生成する複製手段とを有し、前記展開像が前記複製禁止情報と見なされた時に複製動作を停止させる又は行わないように構成している。

10 【0009】また、本発明における第 2 のデータ監視方法は、第 1 のデータ監視方法に、更に、複製が禁止されているデータの複製禁止情報を更新する更新手段を有し、複製禁止情報の変更ができるように構成している。

【0010】また、本発明における第 3 のデータ監視方法は、第 2 のデータ監視方法に、更に、前記データ監視方法は、更に、変更権限の管理情報をもつ更新情報を取得する取得手段を備し、更新情報の内容に応じて、複製禁止情報の変更ができるように構成したものである。

20 【0011】また、本発明における第 3 のデータ監視方法において、前記更新情報は記憶メディアによって提供されるように構成したものである。

【0012】また、本発明における第 3 のデータ監視方法において、前記更新情報は認証確認ができる情報提供媒体によって提供されるように構成したものである。

【0013】また、本発明における第 3 のデータ監視方法において、前記更新情報はネットワークによって提供されるように構成したものである。

30 【0014】また、本発明における第 4 のデータ監視方法は、第 2 のデータ監視方法に、更に、他の情報源に、所定の時間で複製禁止情報を問い合わせる情報自動取得手段と、更新情報の履歴を保存する履歴保存手段とを有し、他の情報源と自ら保有する複製禁止情報とが異なるときに、複製禁止情報を更新するように構成したものである。

【0015】また、本発明における第 5 のデータ監視方法は、第 1 のデータ監視方法に、更に、前記データ監視手段の機能を停止させる解除手段を具備し、認証確認後に複製を停止させる機能を解除できるように構成したものである。

40 【0016】また、本発明における第 6 のデータ監視方法は、像画像を入力する入力手段と、前記像画像を監視するデータ監視手段と、他の情報源に複製禁止情報を問い合わせ、情報を取得する問い合わせ手段とを具備し、前記像画像が前記複製禁止情報と見なされた時に前記像画像の入力を停止させるように構成したものである。

【0017】また、本発明における第 4 のデータ監視方法において、前記データ監視方法はネットワーク上の所定の装置に蓄積された複製禁止情報を問い合わせ、取得するように構成したものである。

50 【0018】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【0019】（第1の実施の形態）まず、本発明の第1の実施の形態で、パーソナルコンピュータにおける不正な複製を禁止するデータ監視方法を組み込む一実施例を図1、図2、図3、図4を用いて説明する。図2はパーソナルコンピュータの使用環境の構成図を示したものである。パーソナルコンピュータ1（以下、パーソナルコンピュータ1をPC1と記述する。）には、様々なアプリケーション・ソフトウェアが搭載され、簡易な印刷システムを構成した場合には編集処理、加工処理、画像処理（色処理）を行う。スキャナ3は画像をPC1に入力するのに使われる。複製手段としてのプリンタ2はPC1の印刷データに従って用紙、OHP用紙等に印字イメージの像形成を行う。PC1はネットワーク100に接続されると、ネットワーク100上のネットワークスキャナ5（以下、NS5と記述する。）から画像を取り込んだり、ネットワークプリンタ4（以下NP4と記述する。）に印刷データを転送して印刷もできる。

【0020】DTPシステムは、色処理、加工を行うPC1、印刷するプリンタ2があれば構成できる。更に、原稿を読み取るのにスキャナ3を接続する。

【0021】次に、図1を用いて、PC1が特定の印刷データ11を印刷する場合の動作を説明する。

【0022】図1はパーソナルコンピュータ1のブロック図である。PC1にインストールされたアプリケーションで印刷イメージが確定すると印刷指定が行われ、印刷データ11が生成される。さらに、印刷データ11はプリンタドライバ12に渡される。プリンタドライバ12は、PC1からプリンタ2にデータの橋渡しを行う制御プログラムとして、予めインストールされているものである。このプリンタドライバ12はアプリケーションより印刷指定された印刷データ11をプリンタ2に転送する。

【0023】データ監視手段としての印刷情報解析回路15は、プリンタ2に転送される印刷データ11を常にモニターし、対象データとしてのページ記述言語などで記載された文字列情報、画像パターン情報、コード情報、電子透かし技術で埋め込まれた暗号情報などを確認メモリ16の中で最終的な展開像に事前に形成し、複製禁止情報14からの情報と照合および解析を行なう。もし、この印刷データ11の印刷情報が予め複製禁止情報14に登録されているものと判定した場合は、プリンタドライバ12に対して印刷データの転送を停止させる停止命令151を出力する。プリンタドライバ12は、停止命令151によって、印刷データの転送を停止する。これによって、不正な印刷をPC1レベルで防止できる。複製禁止情報14の内容は、印刷を禁止したい内容に対し、常に対応して更新できるようにする。これによって、日々変更される機密管理レベル、機密情報、日

新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。

【0024】この更新方法について説明する。更新手段および取得手段としての情報更新回路13は、ICカード200が挿入されると、ICカード200の認証を行う。更新権利があると判定した場合のみ、ICカード200に保存された更新データを取得する。次に、情報更新回路13は、取得した更新データに基づいて、複製禁止情報14の内容を更新する。また、更新データはネットワーク100を経由して入手しても良い。この更新機能を持つことで、禁止印刷情報の更新が簡単に行え、日常的に更新される最新情報に内容を維持することができる。機器に内蔵したメモリ交換が不要なので、更新を迅速に行え、不正印刷の広がりやの拡大を防止できる。

【0025】また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【0026】次に、図3を用いて、複製禁止情報14の格納情報について説明する。図3は複製禁止情報14の格納情報を示した図である。

【0027】複製禁止情報14としては、文書データの文字情報141、画像パターン情報142、コード情報143、画像中に電子透かし技術で挿入された暗号情報144など、文書を特定できる情報が保存されている。

【0028】文書データの文字列情報141には、文書中のタイトル、文書中の特定文字列（例えば、機密文書の主要なキーワードなど）を保存する。画像パターン情報142には、印刷情報を特定できる固有のパターン情報が保存される。コード情報143には、原稿データに文書管理コードが付与される場合に対応するコードの解析情報が保存される。暗号情報144には、著作権で保護された写真画像データに埋め込まれた電子透かし解説情報や、スキャナ3で読み込む原稿に予め所定の暗号化（セキュリティ印刷等）によって印刷されている暗号パターンやの解説アルゴリズム、コードの種別情報などが保存される。複製禁止情報14は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でも良い。

【0029】次に、図4を用いて、印刷情報解析回路15の動作を説明する。図4は印刷情報解析回路15のブロック図である。印刷情報解析回路15は、プリンタドライバ12を常にモニターし、印刷を開始する際に必ず所定の動作を行うようにする。まず、動作を開始すると描画エンジン154は、プリンタドライバ12から印刷データ11の描画情報入手し、確認メモリ16に描画情報に従って描画動作を行う。描画された描画画像データ161は、各種の解析エンジンによって、内容が解析される。描画画像データ161の中のタイトル領域はタイトル解析エンジン155が領域を特定し、その内容の

解析結果を照合回路 159 に転送する。照合回路 159 は複製禁止情報 14の中から、照合情報として使える文字情報 141を選び出し、タイトル解析エンジン 155 が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、信号 151によってプリンタドライバ 12の印刷動作を停止させる。

【0030】同様に、文書解析エンジン 156 はテキスト領域を検出し内容を解析し、イメージ解析エンジン 157 は写真領域を検出し内容を解析し、コード解析エンジン 158 はコード領域を検出し内容を解析する。解析結果は、それぞれ照合回路 159 に転送される。照合回路 159 は複製禁止情報 14の中から、照合情報として使える文字情報 141、画像パターン情報 142、コード情報 143、暗号情報 144をそれぞれ選択し、各種解析エンジンから転送されてくる解析結果と照合する。照合の結果、いずれかの一致検出が発見されると不正印刷の印字と見なし、信号 151によってプリンタドライバ 12の印刷動作を停止させる。また、コード解析エンジン 158 は解読に必要なデコードアルゴリズムを照合回路 159 に問い合わせる最新の解読アルゴリズムを入手できるようにする。これによって、日新月歩する暗号技術に常に対応できる。照合回路 159 は、各解析エンジンからの問い合わせに応じ、複製禁止情報 14の中から必要な情報を入手して各解析エンジンに返答する。

【0031】このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。

【0032】以上、第 1の実施の形態によれば、PC1からプリンタに印刷を行う際に印刷内容を解析し、不正印刷を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金権の偽造などを未然に防ぐことができる。さらに、不正印刷情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。結果、不正印刷の広がり

の拡大を防止できる。

【0033】また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【0034】また、パーソナルコンピュータに不正印刷防止機能を持たせる場合は、特別なハードウェアはいらなく、ソフトウェアのみをインストールすれば良く、低コストで実現できる。

【0035】(第 2の実施の形態) 第 1の実施の形態ではパーソナルコンピュータに不正印刷防止機能を組み込む場合を説明したが、ここではプリンタに不正印刷防止機能を持たせる一実施例を説明する。

【0036】図 2、図 5を用いて、プリンタ 2の動作を

説明する。図 5はプリンタ 2のブロック図である。

【0037】プリンタ 2は PC1からの印刷データを受信バッファ 21で受け、コマンド解析回路 22に順次印刷データを送る。コマンド解析回路 22は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路 22は解析した結果により、文字、図形描画を行う必要があれば、図形/文字描画回路 23に印刷データを転送する。図形/文字描画回路 23は、メモリコントローラ 25を経由して、画像メモリ 26に所定の描画動作を行う。同様に、コマンド解析回路 22は解析した結果により、写真データを展開する必要がある、イメージ描画回路 27に印刷データを転送する。イメージ描画回路 27は、メモリコントローラ 25を経由して、画像メモリ 26に所定の写真データを展開する。メモリコントローラ 25は画像メモリ 26に所望の画像データが形成されるとプリンタエンジン 24に画像データを転送する。プリンタエンジン 24は、受け取った画像データから紙に印刷を行う。

【0038】データ監視手段は、印刷情報解析回路 28と複製禁止情報 29により構成される。印刷情報解析回路 28は、画像メモリに展開される画像データをモニターし、プリンタエンジン 24に画像データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報 29に保存された情報と一致した場合は、信号 281により、プリンタエンジン 24の動作を停止させる。

【0039】次に、更新手段としての更新回路 30について説明する。複製禁止情報 29の内容は、印刷を禁止したい内容に対し、常に対応して更新できるようにする。これによって、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。この更新方法について説明する。更新回路 30は、ICカード 200が挿入されると、ICカード 200の認証を行う。更新権利があると判定した場合のみ、ICカード 200に保存された更新データを取得する。次に、更新回路 30は、取得した更新データに基づいて、複製禁止情報 29の内容を更新する。また、更新データは PC1より入手しても良い。印刷データの他に、定期的、不定期、印刷時でも良いが、更新データを一緒に PC1より送り、受信バッファ 21経由してコマンド解析回路 22が受ける。コマンド解析回路 22は印刷データと別に定義された命令コードから更新データを判定し、信号 221を経由して更新回路 30に更新データを送付する。更新回路 30は更新データに基づき、複製禁止情報 29の保存情報を更新する。更に、ネットワーク 100より PC1を経由して更新データを入手しても良い。

【0040】この更新機能を持つことで、禁止印刷情報の更新が簡単に行え、日常的に更新される最新情報に内容を維持することができる。機器に内蔵したメモリ交換

が不要なので、更新を迅速に行え、不正印刷の広がりの拡大を防止できる。また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【0041】次に、図6を用いて、複製禁止情報29の説明を行う。図6は複製禁止情報29の格納情報を示した図である。複製禁止情報29としては、文書データの文字情報291、画像パターン情報292、コード情報293、画像中に電子透かし技術で挿入された暗号情報294など、文書を特定できる情報が保存されている。

【0042】文書データの文字列情報291には、文書中のタイトル、文書中の特定文字列（例えば、機密文書の主要なキーワードなど）を保存する。画像パターン情報292には、印刷情報を特定できる固有のパターン情報が保存される。コード情報293には、原稿データに文書管理コードが付与される場合に対応するコードの解析情報が保存される。暗号情報294には、著作権で保護された写真画像データに埋め込まれた電子透かし解読情報や、スキャナ3で読み込む原稿に予め所定の暗号化（セキュリティ印刷等）によって印刷されている暗号

パターンの解読アルゴリズム、コードの種別情報などが保存される。複製禁止情報29は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でも良い。

【0043】この複製禁止情報29は、必要な情報を追加するだけで、あらゆる文書、原稿に対応できる。表示システムに本発明のデータ監視方法を導入する際には、動画像情報を追加すれば良く、見せたくない動画の表示も防止する事ができる。表示機能は、ソフトウェア的印刷機能を定義される。よって、ユーザーからみた場合は表示機能も情報を得る手段と解釈すれば印刷機能と同等に扱われる。

【0044】次に、図7を用いて、印刷情報解析回路28の動作を説明する。図7は印刷情報解析回路28のブロック図である。印刷情報解析回路28は、画像メモリに展開される画像データ261をモニターし、画像データ261が形成される際に必ず所定の動作を行うようにする。まず、動作を開始すると各種解析エンジンを用いて画像メモリ26の内容を解析する。画像データ261の中のタイトル領域はタイトル解析エンジン285が領域を特定し、その内容の解析結果を照合回路289に転送する。照合回路289は複製禁止情報29の中から、照合情報として使える文字情報291を選び出し、タイトル解析エンジン285が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、信号281によってプリンタエンジン24の印刷動作を停止させる。

【0045】同様に、文書解析エンジン286はテキスト領域を検出し内容を解析し、イメージ解析エンジン2

87は写真領域を検出し内容を解析し、コード解析エンジン288はコード領域を検出し内容を解析する。解析結果は、それぞれ照合回路289に転送される。照合回路289は複製禁止情報29の中から、照合情報として使える文字情報291、画像パターン情報292、コード情報293、暗号情報294をそれぞれ選択し、各種解析エンジンから転送されてくる解析結果と照合する。照合の結果、いずれかの一致検出が見られると不正印刷の印字と見なし、信号281によってプリンタエンジン24の印刷動作を停止させる。また、コード解析エンジン288は解読に必要なデコードアルゴリズムを照合回路289に問い合わせる最新の解読アルゴリズムを入手できるようにする。これによって、日新月歩する暗号技術に常に対応できる。照合回路289は、各解析エンジンからの問い合わせに応じ、複製禁止情報29の中から必要な情報を入手して各解析エンジンに返答する。

【0046】このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。また、動画像データに対しては、フレーム画像を対象に静止画像エンジンを適用できる。また、動きを含む動画解析エンジンの追加（図示せず）によって、あらゆる動画像にも適用できる。

【0047】以上、第2の実施の形態によれば、プリンタ2の内部で印刷を行う際に印刷内容を解析し、不正複写を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金庫の偽造などを未然に防ぐことができる。さらに、複製禁止情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。結果、不正複写の広がりの拡大を防止できる。

【0048】また、認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

【0049】また、プリンタに不正な複製を防止するデータ監視機能を持たせる場合は、特別な描画エンジン、ハードウェアはいらなく、プリンタコントローラのソフトウェアのみ変更すれば良く、低コストで実現できる。

【0050】（第3の実施の形態）第2の実施の形態ではプリンタに不正な複製を防止するデータ監視機能を組み込む場合を説明したが、ここではスキャナにデータ監視機能を持たせる一実施例を説明する。

【0051】図8を用いて、ネットワークスキャナ5の動作を説明する。図8はネットワークスキャナ5のブロック図である。

【0052】対象となる原稿（図示せず）をイメージセンサ51によって読み取り、A/D変換器52によってデジタル画像データに変換する。ここで、所定のMFT変換、カラー処理等画像処理が画像処理回路53で行わ

10

20

30

40

50

れ、ネットワークインタフェース 54（以下、ネットワーク I/F 54 と記す。）を経由して、画像データの転送が行われる。データ監視手段としての入力情報解析回路 55 は複製禁止情報 56 に保存された情報に基づいて印刷が禁止されている原稿かどうかの判定を行う。もし、禁止されている原稿を検出した場合は、信号 551 によってネットワーク I/F 54 に対し、画像データの転送を停止させる。

【0053】複製禁止情報 56 は図 3 に図示する複製禁止情報 14 と同様のものである。また、複製禁止情報 56 は情報更新回路 57 によって、更新される。ネットワーク上に接続された他の機器からネットワーク I/F 54 を経由して更新データを取得しても良い。さらに、着脱可能なメモリーカード 500 からの更新情報から取得しても良い。メモリーカード 500 の着脱の時に、「更新する」、「更新しない」を情報更新回路 57 が、複製禁止情報 56 と、メモリーカード 500 を照合し、変更の有無から判定する。

【0054】また、複製禁止情報 56 と同様の内容は、登録情報問い合わせ回路 58 によってネットワークを経由して入手することもできる。これによって、膨大な情報を格納するメモリを搭載する必要がなく、製品コストを削減できる。更に、読み取りを行うと、入力情報解析回路 55 が特定のデータベースを自動的に指定し、複製禁止情報 56 と同じ照合データを入手する仕組みを持つ。これによって、ユーザーが都度、更新する必要がなくなる。また、迅速な対応もできる。この自動更新は、他のプリンタ、パーソナルコンピュータにも適用できる。

【0055】なお、スキャナは PC1 に接続されるものでも、同様に本発明のデータ監視機能を組み込むことができる。

【0056】以上、第 3 の実施の形態によれば、ネットワークスキャナ 5 は、複製禁止情報 56 と同様の内容を登録情報問い合わせ回路 58 によってネットワークを経由して入手するので、膨大な情報を格納するメモリを搭載する必要がない。結果、製品コストを削減できる。

【0057】また、読み取りを行うと、入力情報解析回路 55 が特定のデータベースを自動的に指定し、複製禁止情報 56 と同じ照合データを入手する自動更新機能の仕組みを持つので、ユーザーが都度、更新する必要がなくなる。結果、日々変更される機密管理レベル、機密情報、日新月异で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。

【0058】（第 4 の実施の形態）第 3 の実施の形態ではスキャナにデータ監視機能を組み込む場合を説明したが、ここではネットワークプリンタにデータ監視機能を持たせる一実施例を説明する。

【0059】図 9 を用いて、ネットワークプリンタ 4 の動作を説明する。図 9 はネットワークプリンタ 4 のプロ

ック図である。

【0060】ネットワークプリンタ 4 はネットワーク上に接続された機器から印刷データを受け取る。コマンド解析回路 42 はネットワークインタフェース 41（以下、ネットワーク I/F 41 と記す。）を経由して印刷データ、命令コマンドのやりとりを行う。コマンド解析回路 42 は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路 42 は解析した結果により、文字、図形描画を行う必要があれば、図形／文字描画回路 43 に印刷データを転送する。図形／文字描画回路 43 は、メモリコントローラ 45 を経由して、画像メモリ 46 に所定の描画動作を行う。同様に、コマンド解析回路 42 は解析した結果により、写真データを展開する必要があれば、イメージ描画回路 47 に印刷データを転送する。イメージ描画回路 47 は、メモリコントローラ 45 を経由して、画像メモリ 46 に所定の写真データを展開する。メモリコントローラ 45 は画像メモリ 46 に所望の画像データが形成されるとプリンタエンジン 44 に画像データを転送する。プリンタエンジン 44 は、受け取った画像データから紙に印刷を行う。

【0061】データ監視機能は、印刷情報解析回路 48 と複製禁止情報 49 により構成される。印刷情報解析回路 48 は、コマンド解析回路 42 で解釈される印刷データをモニターし、プリンタエンジン 44 に画像メモリ 46 から印刷データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報 49 に保存された情報と一致した場合は、信号 481 により、プリンタエンジン 44 の動作を停止させる。第 2 の実施の形態同様に、印刷情報解析回路 48 は画像メモリ 46 をモニターし解析しても良い。

【0062】次に、更新回路 31 について説明する。複製禁止情報 49 の内容は、印刷を禁止したい内容に合わせて更新できる。これによって、日々変更される機密管理レベル、機密情報、日新月异で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応できる。また、更新回路 31 は、ネットワーク 100 より入手した更新データに基づき、複製禁止情報 49 の保存情報を更新することもできる。

【0063】以上、第 4 の実施の形態によれば、ネットワークプリンタ 4 は、ネットワーク 100 より入手した更新データに基づき、複製禁止情報 49 の保存情報を更新するので、不正な複製を迅速に防止できる。

【0064】（第 5 の実施の形態）第 1 から第 4 の実施の形態ではデータ監視機能を組み込んだ装置について説明したが、ここではデータ監視機能を組み込んだ装置に対して、複製禁止情報を迅速に配信できる方法の一実施例を説明する。

【0065】図 10、図 11 を用いて、印刷を禁止したい情報の登録機能について説明する。図 10 はネットワ

ーク上に接続された機器への登録機能説明図である。図 11 は複製禁止情報登録装置 6 のブロック図である。

【0066】不正な複製を防止するためには、いかに迅速に目的とする複製物を検出し、複製を防止するかが重要である。図 10 に図示する複製禁止情報登録装置 6 はネットワーク 100 上に接続されたネットワークスキャナ 5、ネットワークプリンタ 4、パーソナルコンピュータ 1、第 n のネットワークプリンタ 7 に対して、複製禁止情報をネットワーク経由で配信する装置である。各装置に組み込まれた不正印刷防止機能は、個々に組み込まれた更新手段によって、複製禁止情報登録装置 6 からの更新データを取得し、複製禁止情報の内容を最新のものに更新する。これによって、ユーザに負担をかけることなく、迅速に不正印刷の情報を各機器に伝達でき、不正な複製を未然に防止できる。

【0067】次に、図 11 を用いて、複製禁止情報登録装置 6 の詳細を説明する。図 11 は複製禁止情報登録装置 6 のブロック図である。

【0068】図 11 において、情報設定手段 66 は、記録媒体 150 により複製禁止情報を取得する。

【0069】記録媒体は、FD（フロッピー（登録商標）ディスク）、MO、CD-R 等複製禁止情報を記録できるものであれば良い。また、別な情報取得方法として、キーボードからの入力、スキャナなどによる画像パターンの読み取りなどがある。情報設定手段 66 は、新規な情報が入力されると、禁止印刷登録情報 65 を更新する。禁止印刷登録情報 65 を更新する別な方法としてネットワーク 61 を経由する方法もある。この場合は、登録情報自動更新手段 64 に、予め決められたデータベースを指定して更新データを入手するように設定しておく。更新記録は、更新履歴情報 63 として保存する。履歴情報を保存することで、登録情報自動更新手段 64 が履歴情報 63 から禁止印刷登録情報 65 を更新する必要がある「ある」、「ない」を判定できる。更新周期は所定の時間間隔でも良いし、予め決められたデータベースからの通知によってでも良い。情報開示／配信手段 62 は、ネットワーク 100 を経由した問い合わせに対し、禁止印刷登録情報 65 を開示する。また、管理下に置かれたプリンタ、スキャナ、パーソナルコンピュータに対して禁止印刷登録情報 65 の配信、または更新情報の配信を行う。

【0070】機器側の実施例として、ネットワークプリンタ 4 の場合を説明する。ネットワークプリンタ 4 では、禁止印刷登録情報 65 の配信が複製禁止情報登録装置 6 より行われると、更新回路 31 が更新情報を取得し、複製禁止情報 49 を書き換える。

【0071】また、ネットワークプリンタ 4 には登録情報問い合わせ回路 33 があり、印刷情報解析回路 48 の指示により情報開示／配信手段 62 から直接に禁止印刷登録情報 65 を取得することもできる。

【0072】これによって、装置側は複製禁止情報 49 の保存メモリが不要になり、コストを削減できる。また、禁止印刷登録情報 65 を更新すれば、ネットワークプリンタ 4 も更新されるので、管理がしやすく、迅速な対応ができる。

【0073】更新記録は、更新履歴情報 32 として保存する。履歴情報を保存することで、登録情報問い合わせ回路 33 は無効な問い合わせを防止できる。

【0074】以上、第 5 の実施の形態によれば、複製禁止情報登録装置 6 からネットワークに接続された各機器に対し禁止印刷登録情報 65 を開示／配信できるので、機器管理、機器メンテナンス、機密情報レベルの変更が行いやすい。

【0075】また、一カ所の情報変更で、ネットワーク上の管理された機器を一斉に更新することができるので、迅速に不正な複製を防止できる。

【0076】（第 6 の実施の形態）データ監視機能を組み込んだ装置に対して、不正な複製を防止する機能を解除する方法の一実施例を図 12 を用いて説明する。図 12 は、解除手段としての防止解除設定回路 16 の説明図である。

【0077】装置のメンテナンスや、何らかの都合により、不正印刷の防止機能を解除したい場合がある。機能を解除する権限を有するユーザは解除命令を行うことができる IC カードを防止解除設定回路 16 に挿入する。防止解除設定回路 16 は、IC カードの認証を行い、印刷情報解析回路 15 に機能停止を指示する。これによって、不正な複製を防止する機能を停止できる。

【0078】また、IC カードに代わり、ネットワーク 100 を経由してパスワードによる解除方法や、暗号キーによる解除方法でも良い。いずれにしても、解除権限をもつユーザが特定できる方法であれば良い。防止解除設定回路 16 には、ユーザ認証の登録機能をもち、ネットワーク 100 から設定できる。これにより、組織の変更、機器の移動、機密レベルの変更等、様々な管理状態に迅速に対応できる。

【0079】以上、第 6 の実施の形態によれば、防止解除設定回路 16 を利用することで、機器メンテナンスができる。また、防止解除設定回路 16 はユーザ認証の登録機能をもつので、自在な管理を可能にする。これにより、組織の変更、機器の移動、機密レベルの変更等、様々な管理状態に迅速に対応できる。

【0080】以上、第 1 の実施の形態から第 6 の実施の形態によれば、迅速に不正な複製を防止することができる。

【0081】なお、本発明のデータ監視方法は、CPU、DSP によるソフトウェアによって実現できる。また、専用のハードウェアによって実現しても良い。

【0082】さらには、スキャナ、プリンタ、パーソナルコンピュータ上で、原稿画像データ、文書テキストデ

ータ、暗号データなど様々な特徴のデータに対応できることから、印刷に限らず、モニター表示にも利用できる。

【0083】また、機密文書管理ソフトウェアとしてデータベース、流通システム、電子メール等の文書交換ソフトウェア、ドキュメントの配信ソフトウェアに組み込むことも、もちろんできる。

【0084】また、静止画像にとどまらず、動画画像にも同様に適用でき、動画データ管理にも応用することができる。

【0085】

【発明の効果】以上のように、本発明によれば、複製が禁止された原稿、電子データ等の不正な複製を未然に、かつ迅速に防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態であるパーソナルコンピュータ1のブロック図

【図2】本発明の第1の実施の形態であるパーソナルコンピュータの使用環境の構成図

【図3】本発明の第1の実施の形態である複製禁止情報14の格納情報を示した図

【図4】本発明の第1の実施の形態である印刷情報解析回路15のブロック図

【図5】本発明の第2の実施の形態であるプリンタ2のブロック図

【図6】本発明の第2の実施の形態である複製禁止情報29の格納情報を示した図

【図7】本発明の第2の実施の形態である印刷情報解析回路28のブロック図

【図8】本発明の第3の実施の形態であるネットアークスキャナ5のブロック図

【図9】本発明の第4の実施の形態であるネットワークプリンタ4のブロック図

【図10】本発明の第5の実施の形態であるネットワーク上に接続された機器への登録機能説明図

【図11】本発明の第5の実施の形態である複製禁止情報登録装置6のブロック図

【図12】本発明の第6の実施の形態である防止解除16の説明図

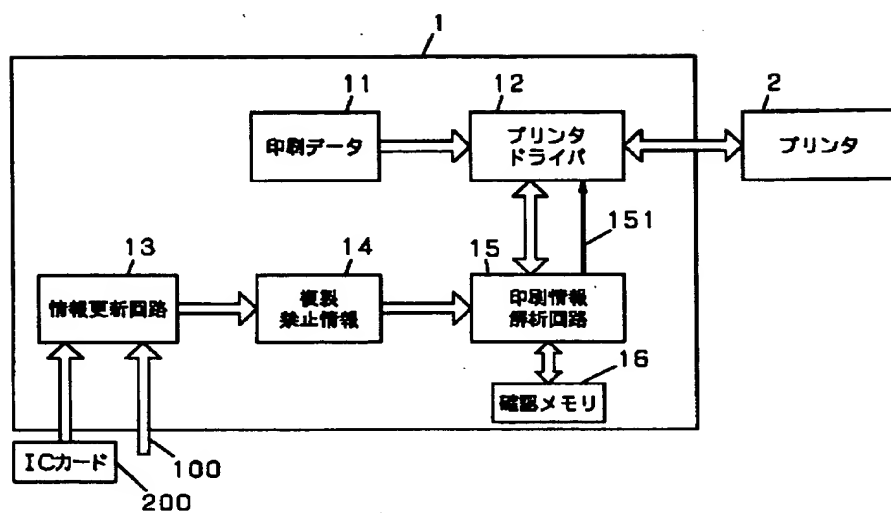
【図13】従来のカラー複写機のブロック図

【符号の説明】

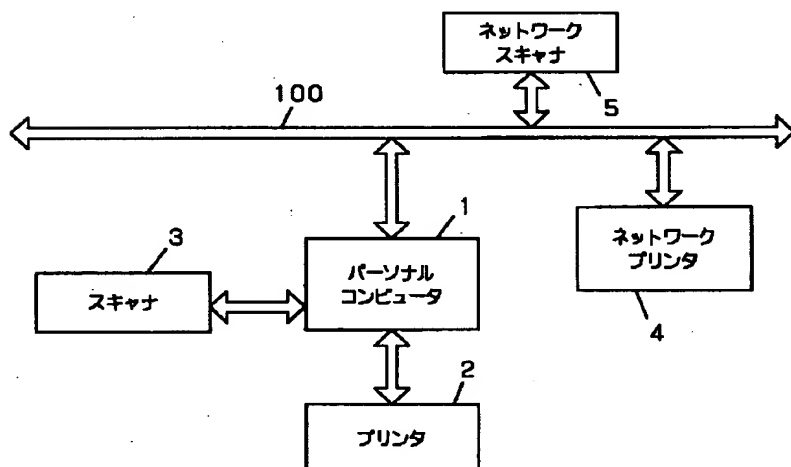
- 1 パーソナルコンピュータ
- 2 プリンタ
- 3 スキャナ
- 4 ネットワークプリンタ
- 5 ネットワークスキャナ
- 6 複製禁止情報登録装置
- 7 第Nのネットワークプリンタ

- 11 印刷データ
- 12 プリンタドライバ
- 13 情報更新回路
- 14 複製禁止情報
- 15 印刷情報解析回路
- 16 確認メモリ
- 17 防止解除設定回路
- 21 受信バッファ
- 22 コマンド解析回路
- 23 図形／文字描画回路
- 24 プリンタエンジン
- 25 メモリコントローラ
- 26 画像メモリ
- 27 イメージ描画回路
- 28 印刷情報解析回路
- 29 複製禁止情報
- 30 更新回路
- 31 更新回路
- 32 更新履歴情報
- 33 登録情報問い合わせ回路
- 41 ネットワークインタフェース
- 42 コマンド解析回路
- 43 図形／文字描画回路
- 44 プリンタエンジン
- 45 メモリコントローラ
- 46 画像メモリ
- 47 イメージ描画回路
- 48 印刷情報解析回路
- 49 複製禁止情報
- 51 イメージセンサ
- 52 A/D変換器
- 53 画像処理回路
- 54 ネットワークインタフェース
- 55 入力情報解析回路
- 56 複製禁止情報
- 57 情報更新回路
- 58 登録問い合わせ回路
- 61 ネットワークインタフェース
- 62 情報開示／配信手段
- 63 更新履歴情報
- 64 登録情報自動更新手段
- 65 複製禁止登録情報
- 66 情報設定手段
- 100 ネットワーク
- 150 記録媒体
- 200 ICカード
- 500 メモリカード

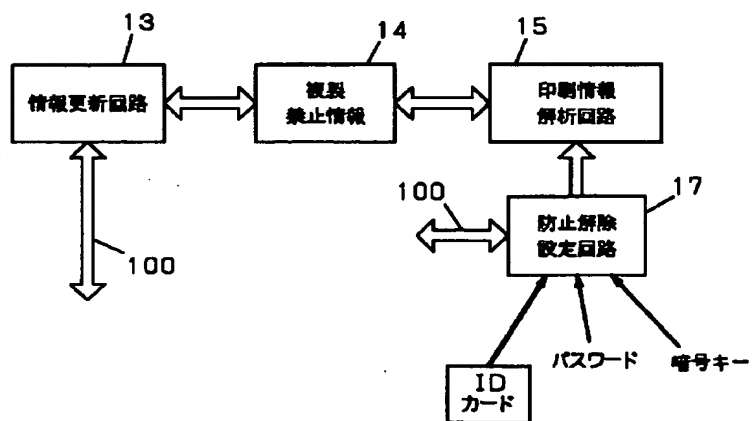
【図 1】



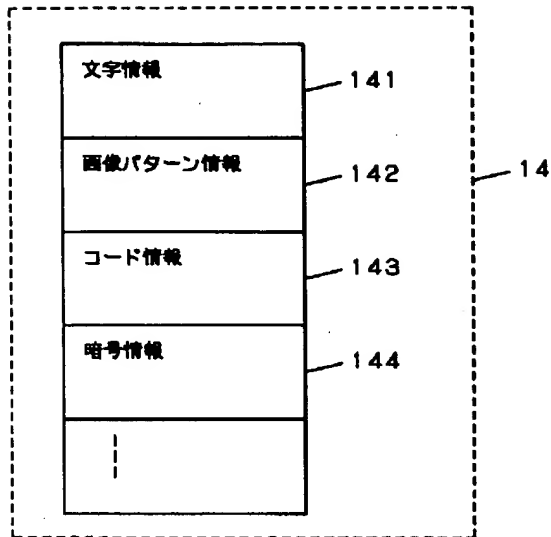
【図 2】



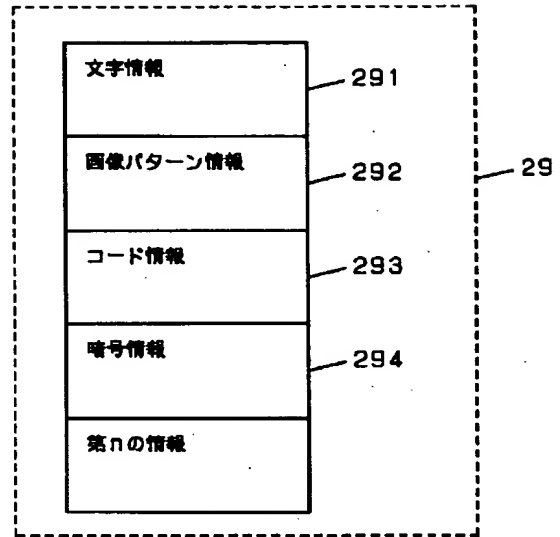
【図 12】



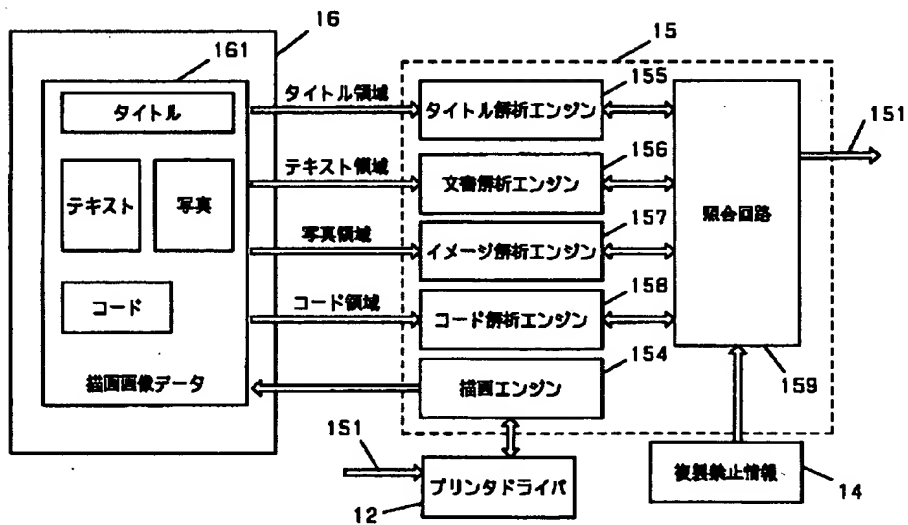
【図 3】



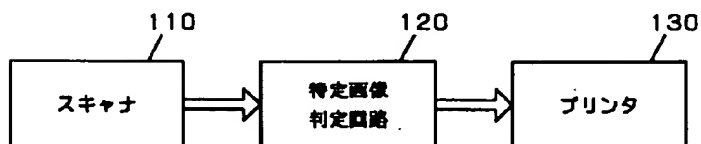
【図 6】



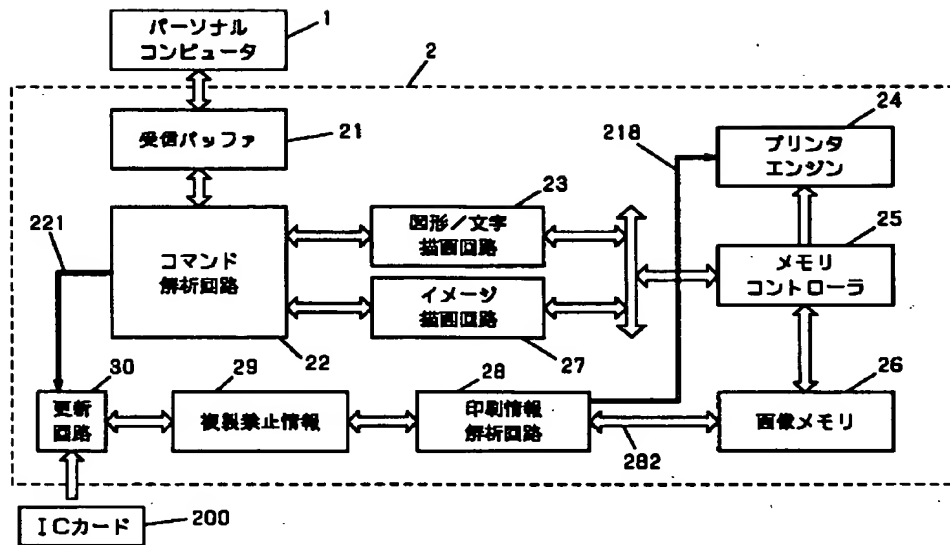
【図 4】



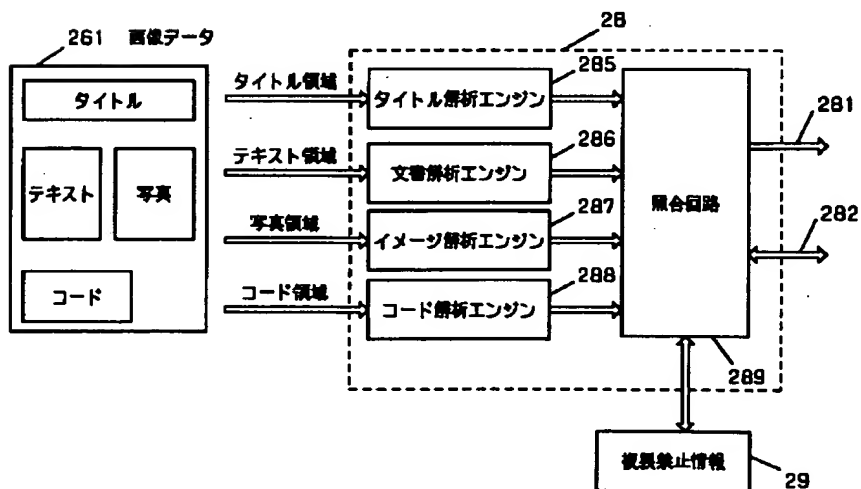
【図 13】



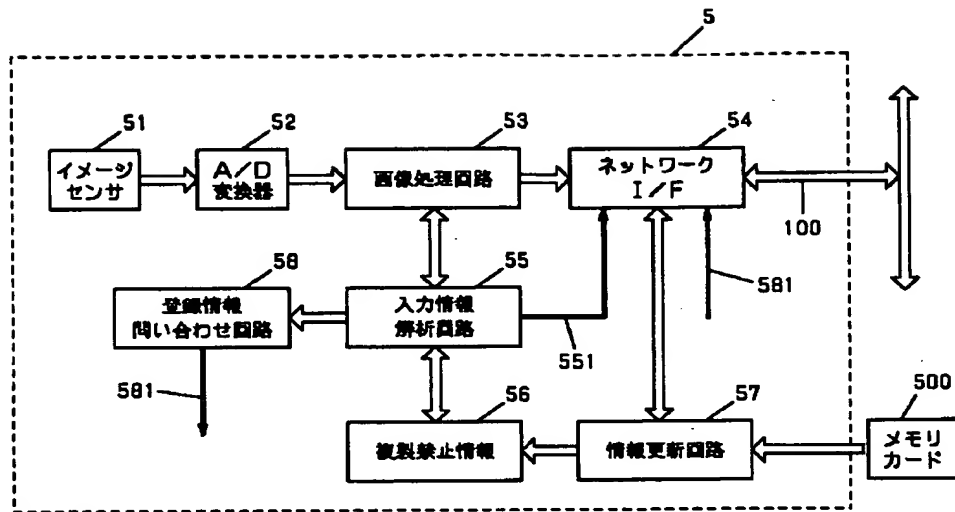
【図 5】



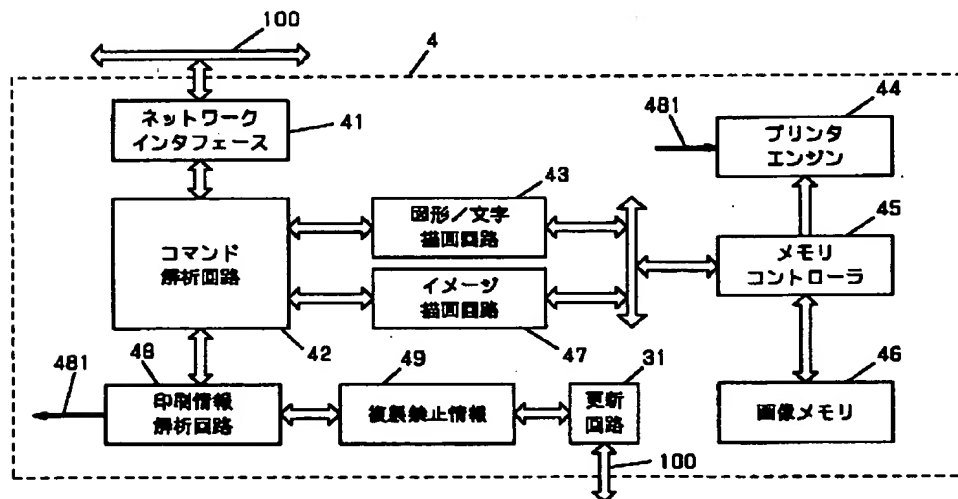
【図 7】



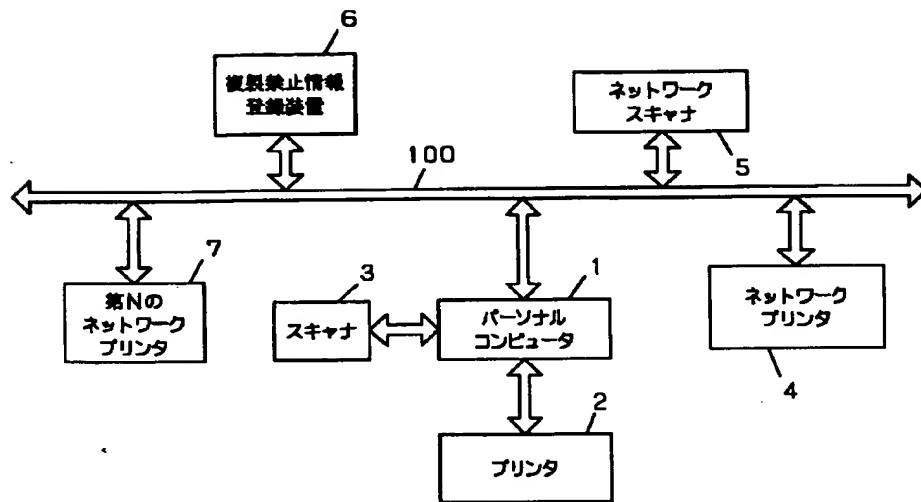
【図 8】



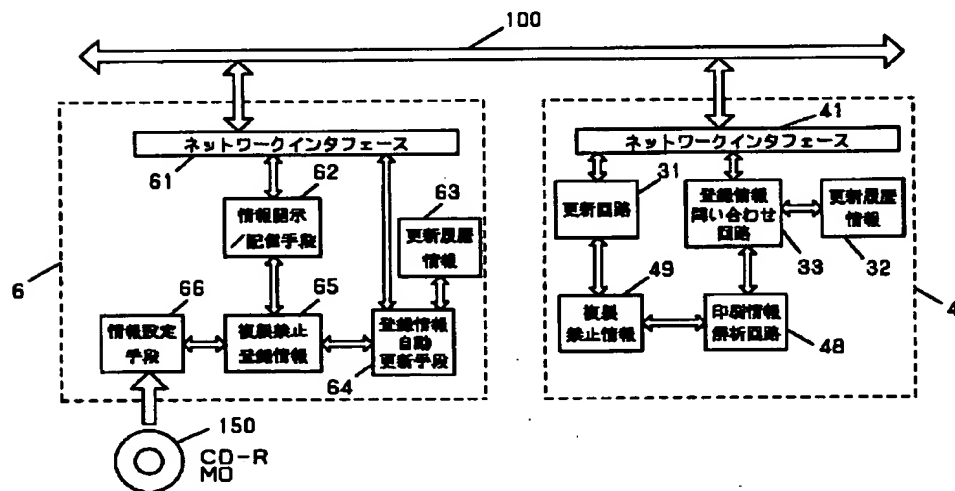
【図 9】



【図10】



【図11】



フロントページの続き

(72)発明者 渡辺 辰巳
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 2H034 FA01
5B021 AA01 CC05 EE01 NN01
5B082 EA07 GA11
5B089 GA21 JA35 JB16 JB22 KA04
KA12 KG10 LB12 MC08
5C077 LL14 NP07 PP55 PP65 PQ08
PQ20 PQ22